UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/532,434	04/22/2005	Unho Choi	8739.098.00	9122

30827 7590 05/18/2010
MCKENNA LONG & ALDRIDGE LLP
1900 K STREET, NW
WASHINGTON, DC 20006

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
05/18/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/532,434	CHOI, UNHO	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 March 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *28,30-38,40-42,44-48 and 75-80* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *28, 30-38, 40-42, 44-48, and 75-80* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

The instant application having Application No. 10/532434 is presented for examination by the examiner. Claims 28, 30-38, 40-42, 44-48, and 75-80 are pending. Claims 28, 30-38, 40-42, and 44-48 have been amended.

Response to Amendment

Claim Objections

Claim 43 has been canceled, rendering the claim objection moot.

Response to Arguments

Applicant's arguments with respect to claims 28 and 38 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 28, 30, 33-34, 36-38, 40, and 44, 45, 47, 48, 79, and 80 are rejected under 35 U.S.C. 103(a) as being unpatentable over USP 7,325,252 to Bunker et al., hereinafter Bunker in view of USP Application Publication 2003/0212908 to Piesco.

As per claims 28 and 38, Bunker teaches a computer emergency response system linked to a plurality of computer systems, the system comprising:

an information section configured to collect system information and security information related to a security incident that is a threat to at least one of the plurality of computer systems (col. 3, lines 24-28);

a test bed configured to perform an attack simulation for the at least one computer system based on the system information and security information, under conditions similar to those of the at least one computer system (col. 4, lines 5-15); and

an assessment section configured to assess the security incident based on the simulation (col. 4, lines 17-30).

Bunker is silent in explicitly disclosing the attack simulation is performed at the test bed. Piesco teaches performing an attack simulation at a test bed (simulated network environment; 0015, 0019, and 0020). Bunker teaches performing the simulated attacks on the actual network. Piesco teaching of simulating attacks on a simulated network instead of the real network allows real-time analysis without having actual network devices present and tied up (0033). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of

Piesco with Bunker in order to efficiently run a multitude of simulated attacks without actually tying up the resources.

As per claims 30 and 40, Bunker teaches the assessment section assesses the security incident by classifying the incident into of several levels of attack (col. 4, lines 50-55 and col. 7, lines 35-45).

As per claims 33 and 44, Bunker teaches the assessment section is further configured to provide a test scenario for the attack simulation to the test bed (col. 4, lines 60-65), including a method of attack and frequency of attack (col. 4, lines 5-10).

As per claims 34 and 45, Bunker teaches the assessment section is further configured to provide additional test scenarios for the attack simulation to the test bed until the security incident has been simulated on each of the plurality of computer systems (col. 4, lines 10-15).

As per claim 36, Bunker teaches a warning section configured to issue an alert to the at least one computer system based on the assessment of the security incident by the assessment section (col. 4, line 60), wherein the alert includes steps for responding to the security incident [countermeasures; col. 4, lines 62-66).

As per claims 37 and 48, Bunker teaches a warning section configured to issue a forecast to the simulated computer system based on an assessment of the one or more security incidents by the assessment section (col. 4, lines 60-65 and col. 5, line 5).

As per claim 47, Bunker teaches a warning section configured to issue an alert to the at least one computer system based on the assessment of the security incident by the assessment section (col. 4, line 60), wherein the alert includes steps for responding to the security incident in real time [countermeasures; col. 4, lines 62-66).

As per claim 79, Bunker teaches a training section configured to generate training data based on the attack simulation, the training data configured to train the at least one computer system to prevent the security incident; and an information sharing section configured to transmit the training data to the at least one computer system [early warning generators; col. 19, lines 49-65].

As per claim 80, Bunker teaches a warning section configured to issue an alert to the at least one computer system based on the assessment of the security incident by the assessment section, wherein the alert includes steps for preventing the security incident (col. 19, lines 52-55).

Claims 31, 32, 41, 42, and 76-78 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bunker and Piesco as applied to claim 28 and 38 and in further view of USP Application Publication 2002/0199122 to Davis et al., hereinafter Davis.

As per claims 31 and 41, Bunker is silent in explicitly disclosing an evaluation section configured to calculate expected damages from an attack based on at least one security incident with a similar level of attack. Bunker teaches many types of threat assessments and generating details analysis of those threats to the system. Davis teaches an evaluation section configured to calculate expected damages from an attack based on at least one security incident with a similar level of attack (0025 and 0033). This detailed report is just another analysis of the potential a threat may incur to a system. This claim would have been obvious because substituting known method with produce predictable results without changing the original intention is within the ordinary capabilities of one of ordinary skill in the art. Substituting or adding another type of assessment to the vulnerability report is obvious.

As per claims 32 and 42, Bunker is silent in explicitly teaching an asset recovery section configured to provide an expected recovery time from the attack for at least one of the plurality of computer systems. Bunker teaches many types of threat assessments and generating details analysis of those threats to the system. Davis teaches an asset

recovery section configured to provide an expected recovery time from the attack for at least one of the plurality of computer systems (0025 and 0033) as being able to determine the elapsed time between when a vulnerability was introduced and the time a solution was fixed. Adding this into the report is yet another assessment detail which would provide a network administrator valuable knowledge pertaining to vulnerability assessment. Examiner supplies the same rationale to combine Bunker and Davis as recited in the rejection of claims 31 and 41. Substituting or adding another type of assessment to the vulnerability report is obvious.

As per claim 76, Bunker and Piesco are silent in explicitly teaching the evaluation section is further configured to calculate the expected damages in categories of network exposure, system exposure, system service delay, and network service delay. Davis teaches this limitation in Figure 2 and paragraphs 0030-0031 as way to break down and show network damages and system damages. Examiner supplies the same rationale to combine Bunker and Davis as recited in the rejection of claims 31 and 41. Substituting or adding another type of assessment to the vulnerability report is obvious.

As per claim 77, Bunker and Piesco are silent in explicitly teaching the evaluation section is further configured to calculate the expected damages in categories of root authority acquisition, data release, and data forgery. Davis teaches the evaluation section is further configured to calculate the expected damages in categories of root authority acquisition [root break-in], data release [account compromise lead to data

theft], and data forgery [account break-in, forgery of the user] (0030). Examiner supplies the same rationale to combine Bunker and Davis as recited in the rejection of claims 31 and 41. Substituting or adding another type of assessment to the vulnerability report is obvious.

As per claim 78, Bunker teaches an information sharing section configured to transmit the expected damages to the at least one computer system (col. 19, lines 1-15).

Claims 35, 46, and 75 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bunker and Piesco as applied to claim 28 and 38 and in further view of USP Application Publication 2008/0016569 to Hammer et al., hereinafter Hammer.

As per claims 35 and 46, Bunker teaches transmitting the classified security information and the assessment to at least one computer system (col. 4, lines 59-62). Bunker and Piesco are silent in teaching classifying the security information according to a method of attack, time of attack, frequency of attack, internet protocol address of a source of the attack, internet server provider of the source of the attack, and country of origin of the source of the attack. Hammer teaches the above limitations (0012 and 0015) a means of classifying security incidents. Bunker teaches classifying security events and Hammer just teaches more ways in which security incidents can be

classified. The claims are obvious because one of ordinary skill in the art can combine known teachings which produce predictable results.

As per claim 75, Bunker teaches an information sharing section configured to transmit the classified security information and the attack assessment to the at least one computer system (col. 19, lines 1-15).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431